PRIVACY IMPACT ASSESSMENT

Name of System/Application: Business Development Management Information System (BDMIS)
Program Office: Office of Business Development, Government Contracting and Business Development (GCBD), SBA

Once the Privacy Impact Assessment is completed and the signature approval page is signed, please submit an electronic copy and hardcopy with original signatures of the PIA to the SBA Senior Advisor to the Chief Privacy Officer in the Information Privacy Office of the OCIO.

A. CONTACT INFORMATION

1) Who is the person completing this document?

Lawrence Gottlieb, BDMIS Project Manager
Office of Business Development, GCBD
202-205-6032
Lawrence.gottlieb@sba.gov

2) Who is the system owner?

Calvin Jenkins, Deputy
GCBD
202-205-6459
Calvin.jenkins@sba.gov

3) Who is the system manager for this system or application?

LeAnn Delaney, Director (Acting)
Office of Business Development, GCBD
(202) 205-6731
Leann.delaney@sba.gov

4) Who is the IT Security Manager who reviewed this document?

David McCauley, Chief Information Security Officer, Office of the Chief Information Officer
202-205-7103
David.mccauley@sba.gov

5) **Who is the Senior Advisor who reviewed this document?**

Ethel Matthews, Senior Advisor to the Chief Privacy Officer
Office of the Chief Information Officer
202-205-7173
Ethel.matthews@sba.gov

6) **Who is the Reviewing Official?**

Paul T. Christy, Acting Chief Information Officer /Acting Chief Privacy Officer,
Office of the Chief Information Officer
202-205-6708
paul.chrtisty@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) ***Does this system contain any information about individuals? If yes, explain.***

Information is gathered from public individuals to complete standard forms required for application to the 8(a) Business Development Program and the yearly Annual Review re-certification process. This data is entered into electronic versions of the forms via a secure web interface. The information is maintained in a database, as well as transferred to PDF facsimiles of the forms, which are printed, signed and mailed to the SBA.

For initial certification in the 8(a) program the following information is required from public individuals:
Owners Name (including, Tribal Entity Name, Alaska National Corporation Name, Native Hawaiian Organization Name, Community Development Corporation Name, if applicable) Birth Date, Address, Tax ID Number, SSN, EIN, Email Address, Primary North American Industry Classification Code (NAIC), Date Firm Established, Type of Business, Three Years Business Income Tax Records, Two Years Personal Business Income Tax Records, Owner Ethnicity, Gender, Duns Number, Business Legal Structure, Articles of Incorporation, Operating Agreement, By-laws, Stockholder and Board Member Meeting Minutes,
Partnership Agreement, Articles of Organization, Fictitious Business Name filing, and bank signature cards, Business Ownership Percentage, Personal Net Worth, Personal Assets and Liabilities, Owners Net Compensation, Business Revenues, Business Assets and Liabilities and proof of US Citizenship.
Personal Resume, including the education, technical training and business and employment experience (employer's name, dates of employment and nature of employment), including the individual's current duties within the applicant firm.

Names and addresses of any note-holders (e.g., loans from banks or any other parties) are also required.

For continuing eligibility in the 8(a) program (i.e., the Annual Review), the following information is required from public individuals: For a period of 9 years, any changes to the above data, as well as rolling 3 years revenue data derived from their business attributed to 8(a) and non-8(a) contract sources.

a. Is the information about individual members of the public?

Yes. This information is collected from US citizens who own small businesses, and wish to obtain certification in the 8(a) Business Development Program of the US Small Business Administration. For continued eligibility in the 8(a) program, the information is obtained from individuals already certified in the program and reviewed annually by the SBA.

b. Is the information about employees?

No information from SBA employees is collected by BDMIS.

2) What is the purpose of the system/application?

The 8(a) Certification process and related federal statute(s) were established by Congress to assist American citizens who own small businesses and belong to certain designated groups considered socially and economically disadvantaged. This assistance is intended to help these individuals overcome deeply entrenched social and economic obstacles to their success by providing limited preference in the federal procurement process. The 8(a) Certification process is the vehicle that allows individual small business owners to obtain eligibility for this preference. The eligibility lasts 9 years, during which time an Annual Review process is carried out by the SBA to ensure that the applicant meets the statutory and regulatory criteria for continued participation in the program. It involves the same individuals, data and related security issues.

Processes supporting the SBA's 8(a) Business Development program were either paper-based or resided on separate systems on disparate technical platforms. The challenge was to: 1) to automate the remaining paper-based processes, 2) unify functionality and data, to the extent possible, on a single system and 3) provide urgently needed new functionality to improve productivity and ease of use for the user community. The user community consists of: 1) firms applying for the 8(a) program (potentially, an additional increment of thousands of users), 2) specialized SBA staff that processes these applications, 3) already certified firms (these must be re-certified each year they are in the program, for a total potential 9 years; currently approximately 8000 firms) and 4) SBA District Office staff who process the annual 8(a) program re-certifications (approximately 150 users in 60 different locations).

The IT solution consisted of a consistent, completely integrated web-based system for the entire 8(a) Program life-cycle that shares the same user-interface, access method, and data.

Specific features include:

- New electronic interface for the public to apply for 8(a) status via the internet.
- The new system is based on the actual OMB approved forms, similar to the process reflected in Turbo-Tax, and provides a much more user-friendly and intuitive environment than the prior system.
- This interface provides the user with an easy-to-use and interactive user interface that dynamically provides instructions as they are needed.
- The new system meets the requirements of the SBA General Counsel and Inspector General for legally tying the data in the system to the firm applicant/owners and for requiring key supporting documentation in hard copy.
- New and improved interface for the 8(a) processing unit, the so-called 'Central Office Duty Stations', in Philadelphia and San Francisco.
- Completely new public internet interface for the already certified firm to enter data and complete the required forms for their 8(a) Program Annual Review.
- The returning firm logs on with the secure userid they received when they completed their on-line certification.
- The interface is identical to the one they used for entering their certification data, so it is familiar and easy to use.
- Required supporting documentation is clearly spelled out via an on-line checklist.
- Completely new interface for the District Offices to perform the Annual Reviews of the firms in their 8(a) portfolios.
- Integrates tightly with and provides instant access to all current data and forms submitted by the firm, as well as all historical data and forms.
- Contains District Office approved tools for analysis.
- Provides a strict approval workflow for the recommendation process, via BDS, ADD and DD, for all pertinent recommendations, e.g. Retain in Program, Terminate, Graduate, etc.
- Keeps detailed record of all transactions and recommendations
- Notifies approvers via email of pending Annual Review in their approval queue
- Sends pdf version of approval/denial letter to firm when Annual Review is approved by the District Director
- Full-featured ad hoc reporting, giving the ability of the user to query any data field in the system and dump the results into an Excel spreadsheet for further manipulation and analysis.

3) Is the system in the development process?

No.

4) How will the technology investment (new or updated) affect existing privacy processes?

The precursor system to BDMIS was built on the same technology platform, so the privacy processes have not changed.

5) What legal authority authorizes the purchase or development of this system/application?

Sections 7(j), 8(a) and 8(d) of the Small Business Act of 1953 (Public Law 85536) As amended, and as recorded in CFR 13, Part 124.

6) Privacy Impact Analysis: What privacy risks were identified and describe how they were mitigated for security and access controls?

Unauthorized Access to Data
All SBA employees are required to obtain a Public Trust Security Clearance (see OPM Form 85P for details), which includes an exhaustive background check conducted by specialized professionals. Direct access to the system is limited by User ID's and password controls managed via the SBA's General Login System. Access via GLS is provided by the SBA Office of IT security upon receipt of a written request by the user and duly approved by an authorized SBA manager. Further access to data, once the user is admitted to the system, is regulated via access roles and profiles associated with each User ID.

Unauthorized Browsing of data by Authorized Users
Each user is required to have a role in the certification and/or annual review workflow (Roles are defined below in Section 8.1 below), as well as an individual system profile. Access to data, screens, functions and reports is a function of the user's role in the workflow and his/her individual profile. In addition, with the exception of executive level roles (such as System Administrator, Associate Administrator for Business Development, Assistant Administrator for Certification and Eligibility and the Business Opportunity Assistant), access to information for a given role is limited to a specific Office Code.

Downloading Data from System
The system produces an excel extract on demand of any data fields in the system. Access is limited to specific office codes according to role and subject to all the restrictions listed above. After use, any downloaded data is stored on hard-drives in SBA-configured PC's that are password protected, according to SBA standards, and/or in locked file cabinets. Only authorized individuals have keys to these file cabinets. These procedures comply with SOP 90 47, to ensure that data is secured after download.

Access Control

The controls operate at two levels. First, access to the system is limited by userid and password, which keeps the general public from entering the system. Second, an individual with authority to access the system has his/her access limited to the roles defined in a profile tied to his/her specific userid. Training on Privacy Act rules and prohibitions on the dissemination or use of nonpublic information is mandatory and ongoing for SBA staff and contractors. Agency network logon procedures mandate viewing and acknowledgement of a posted Privacy notice prior to entry. SBA Privacy Act System of Records defines routine uses of this information and serves as a control by defining acceptable uses.

SBA maintains Internal Management Controls through periodic auditing from the Office of the Inspector General and the Office of Program Review. Certification and Accreditation of the system is provided by the Chief Information Office and includes a System Security Plan, Risk Assessment, and Security Test & Evaluation every 3 years for existing systems and each instance the system is upgraded or enhanced.

C. SYSTEM DATA

1) What categories of individuals are covered in the system?

This information is collected from US citizens, tribal entities, Alaska National Corporations, Native Hawaiian Organizations and Community Development Corporations who own small businesses, and wish to obtain certification in the 8(a) Business Development Program of the US Small Business Administration. For continued eligibility in the 8(a) program, the information is obtained from individuals already certified in the program and reviewed annually by the SBA.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

This information is collected from US citizens, tribal entities, Alaska National Corporations, Native Hawaiian Organizations and Community Development Corporations who own small businesses, and wish to obtain certification in the 8(a) Business Development Program of the US Small Business Administration. For continued eligibility in the 8(a) program, the information is obtained from individuals already certified in the program and reviewed annually by the SBA.

Also:

Tribal Entities

Alaska National Corporations

Native Hawaiian Organizations

Community Development Corporations

b. What Federal agencies are providing data for use in the system?

The Central Contractor Registry (CCR) This system is managed by GSA and a component of the Integrated Acquisition Environment that is controlled by the U.S. Department of Defense. Central Contractor Registration (CCR) is the primary contractor registrant database for the U.S. Federal Government. CCR collects, validates, stores and disseminates data in support of agency acquisition missions. According to the FAR 4.11, prospective vendors must be registered in CCR prior to the award of a contract; basic agreement, basic ordering agreement, or blanket purchase agreement.

Initial information is loaded by the applicant into to the Central Contractor Registry (CCR) and uploaded within 72 hours to the 8a certification system. The applicant is then provided a Transaction Personal Identification Number (TPIN), which enables him/her to enter the 8(a) SDB Application/Certification System via the SBA General Login System (GLS). The latter manages user access to all mainstream SBA applications.

All subsequent information required for certification required by the 8a/SDB certification system is provided directly by the applicants with one exception: the applicants are required to sign and submit forms that request copies from the IRS of federal tax returns for the last three years. These copies are forwarded directly from the IRS to the Office of Business Development of the SBA.

c. What Tribal, State and local agencies are providing data for use in the system?

NONE. All data is provided by private individuals and/or non-public sector entities.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

For initial certification in the 8(a) program the following information is required from public individuals:

Owners Name (including Tribal Entity Name, Alaska National Corporation Name, Native Hawaiian Organization Name, Community Development Corporation Name, where applicable), Birth Date, Address, Tax ID Number, SSN, EIN, Email Address, Primary North American Industry Classification Code (NAIC), Date Firm Established, Type of Business, Three Years Business Income Tax Records, Two Years Personal Business Income Tax Records, Owner Ethnicity, Gender, Duns Number,

Business Legal Structure, Articles of Incorporation, Operating Agreement, By-laws, Stockholder and Board Member Meeting Minutes,
Partnership Agreement, Articles of Organization, Fictitious Business Name filing, and bank signature cards, Business Ownership Percentage, Personal Net Worth, Personal Assets and Liabilities, Owners Net Compensation, Business Revenues, Business Assets and Liabilities and proof of US Citizenship.
Personal Resume, including the education, technical training and business and employment experience (employer's name, dates of employment and nature of employment), including the individual's current duties within the applicant firm.
Names and addresses of any noteholders (e.g., loans from banks or any other parties) are also required.

For continuing eligibility in the 8(a) program (i.e., the Annual Review), the following information is required from public individuals, as above: For a period of 9 years, any changes to the above data, as well as rolling 3 years revenue data derived from their business attributed to 8(a) and non-8(a) contract sources.

3) Accuracy, Timeliness, and Reliability

Accuracy and timeliness of personal data is optimized by allowing applicants to correct the personal information they provide in the system until completion of the initial application for certification. They also have multiple opportunities to update and correct personal information later in the program, when entering data in the system for the Annual Review, which occurs on a yearly basis for a period of 9 years. Further, individuals may request access to or correction of their personal information pursuant to the procedures outlined in this PIA and in accordance with the Privacy Act.

Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled at a high-security facility in Ashburn, VA. This access is regulated by a 24-hour manned security desk at the entrance to verify photo IDs, reinforced doors that respond only to positive identification via magnetic proximity badges, and 24-hour video surveillance of the entire facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

a. How is data collected from sources other than SBA records verified for accuracy?

A prospective user of BDMIS is asked to enter his/her firm's DUNS and EIN (corporate tax ID number) in his/her request for a userid and password for secure access to the system. These data elements are then matched against the corresponding entries for the firm in the Central Contractor Registration database. Registration in CCR is a regulatory pre-requisite to admission to the 8(a) Program. If these elements do not match

EXACTLY, the firm is not given a userid and password, and, hence, does not gain access to BDMIS. This matching process provides positive identification of the firm and the user to the system.

b. How is data checked for completeness?

The data entry fields in BDMIS correspond to the actual fields in the required OMB-approved forms for applying for certification in the 8(a) program. Before allowing the user to submit his/her data to the SBA, and thus complete the on-line application process, the system checks each field for accuracy. If one or more fields are missing an entry, or contain the wrong type of input (alpha v. numeric), the fields are flagged and the user is notified of the nature of the errors. He/she must correct the errors before the system will allow him/her to submit the totality of his forms and data on-line to the SBA, and thus complete his application for 8(a) certification.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Accuracy and timeliness of personal data is optimized by allowing applicants to correct the personal information they provide in the system until completion of the initial application for certification. They also have multiple opportunities to update and correct personal information later in the program, when entering data in the system for the Annual Review, which occurs on a yearly basis for a period of 9 years. Further, individuals may request access to or correction of their personal information pursuant to the procedures outlined in this PIA and in accordance with the Privacy Act.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in detail in the BDMIS Data Dictionary, which can be found this address:

http://collab.sba.gov/sites/GCBD/OBD/BDMIS/Key%20Project%20Documents/Data/BDMIS%20Data%20Model%20Report%2011-10-09.mht

4) Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for the types of information collected?

General unauthorized access to private information

All initial access to the system is managed by the General Login System of the SBA, which meets all applicable statutory and regulatory conventions for data security and privacy. Once admitted to the system, user access is restricted to the information defined by the specific role assigned to the user. All access and transactions in the system are posted to an audit log, and any infractions of information security rules will be addressed appropriately. All SBA and assigned contractor staff receive SBA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuse.

Unauthorized access from the public internet

Access from outside the SBA (ie, from the public internet, beyond the SBA security 'firewall'), is protected by the SBA General Login System security front-end. This front-end requires a unique userid and password, which is accorded to the user only after he/she has completed a full personal profile which includes a valid DUNS and EIN for the firm. The latter two numbers are dynamically checked with CCR before the user receives his/her userid and password from GLS.

Unauthorized access by SBA staff, e.g., behind the SBA security 'firewall'

Employees or contractors are assigned roles for accessing the system based on their function. SBA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained on information security when they join the organization and periodically thereafter. The Information Systems Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

Access to data is strictly regulated according to the role assigned to a particular SBA employee in the system.

Access to data is restricted by the role and office code of the user in the system. Valid roles include the following:

- System Administrator (ADM): Full control of the application, for maintenance and security purposes. The Sys Admin can see all data for all applicants. He/she CANNOT see the password of the user, or re-set it. Only the user can perform the latter function.
- Assistant Administrator for Business Development (AA/BD): This user makes the final eligibility determination on 8(a) applicants. The role can see all data for all applicants.
- Assistant Administrator for Certification and Eligibility (AA/CE): This user makes the final eligibility recommendation on 8(a) applicants, following the recommendation from the Central Office Duty Station (CODS) Chiefs (see below). This user can see data for all applicants.
- CODS Chief (CC): This role is responsible for assigning new 8(a) applications to the OCEBOS (see below). There are two CODS, whose respective geographic responsibilities loosely correspond to the eastern and western halves of the United States. Each CODS Chief can only see data for applicants in his/her geographic area of responsibility.

- Office of Certification and Eligibility Business Opportunity Specialist (OCEBOS) This user is assigned applications to review by the CODS Chief in his/her area of geographic responsibility. The OCEBOS reviews and analyzes a firm's application to determine if the firm meets the criteria for acceptance in the 8(a) Program. Upon completion of his/her review and analysis, he/she makes a recommendation to the AA/CE to either approve or decline the firm's application. The OCEBOS can only see data for the firms assigned to him/her by the AA/CE.
- Office of the General Counsel (OGC): This user examines the legality of any applications in question, and provides an additional recommendation on whether or not they qualify for certification. This user can only see data for firms that are formally referred to him/her for review by the AA/CE or AA/BD.
- Office of Hearing and Appeals (OHA): This user reviews applications which receive an initial decline and a decline after reconsideration who request an appeal within the appropriate time frame. This user can only see data for firms that are formally referred to him/her for review by the AA/CE or AA/BD.
- Field Office (8ASDBFieldOffice): This is a local District Office user who can see only the approved 8(a) applications for firms located in his/her district.
- District Office Roles. Can only see data for firms in their geographic area of responsibility, i.e., their district.
    1. Business Development Specialist (BDS): Makes initial review an analysis of data entered in system by firm for their Annual Review. Makes first recommendation, which goes up the approval chain to Assistant District Director (ADD)
    2. Assistant District Director: Receives Annual Review recommendation from BDS, approves recommendation and forwards it to District Director for final approval, or vetoes BDS recommendation and makes different recommendation, or sends original recommendation back to BDS for re-work and new recommendation.
    3. District Director: Receives Annual Review recommendation from ADD and ratifies it with final decision, or changes and/or sends it back to ADD for re-work and new recommendation.

D. DATA ATTRIBUTES

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Only that data is collected which is required to complete the forms required for initial 8(a) certification and the yearly Annual Review. These forms and their content are described and mandated by statute in the Code of Federal Regulations (13 CFR 124) and the relevant SBA SOP (SOP 80 05 03). The process of initial certification and yearly Annual Review cannot take place in the absence of any of this data. Most of the data is used to determine that a firm is eligible to participate and remain in the program on the basis of , inter alia, 1) Social and economic disadvantage of the majority owner(s), 2) verified US citizenship of the majority disadvantaged owner(s), 3) demonstrated control of the firm by the majority disadvantaged owner(s), and 4) a means test showing net worth below a certain threshold for the majority disadvantaged owner(s) and spouse(s). In the absence of this data, the program would be vulnerable to fraud.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Data is not formally subject to 'derivation' or 'aggregation. All data queries and reports are ad hoc. All data fields in the system are subject to query. With the proper authority, data fields corresponding to specific date ranges may be downloaded to Excel spreadsheets for further analysis.

3) **Will the new data be placed in the individual's record?**

N\A. No data is formallyderived or aggregated.

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?**

N\A. No data is formally derived or aggregated.

5) **How is the new data verified for relevance, timeliness and accuracy?**

NA. No data is formally derived or aggregated.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

NA. No data is formally derived or aggregated.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If process are not be consolidated please state, "N/A".**

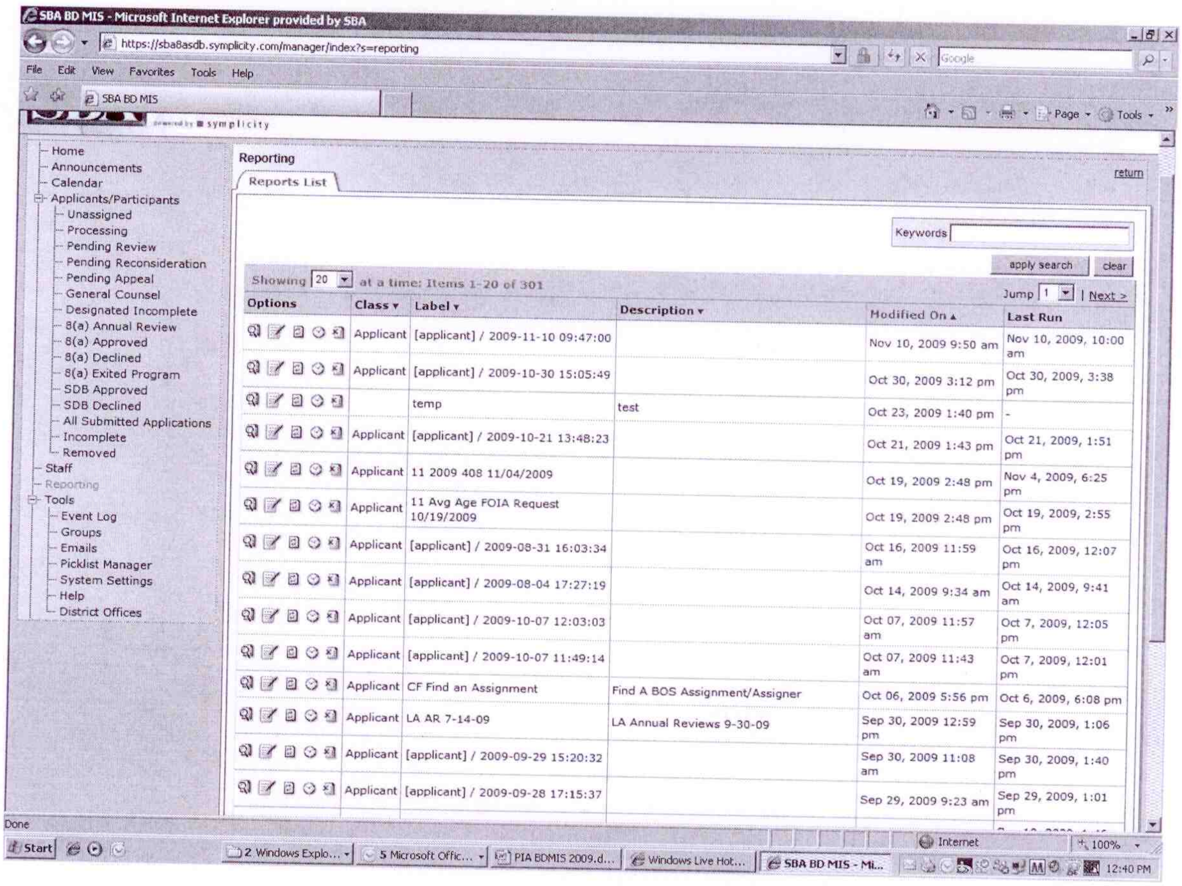
NA. No data is formally derived or aggregated.

8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

N\A. No data is formally derived or aggregated.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reporting is ad hoc. There are no pre-defined or 'canned' reports. With full authority, any data element can be queried over any range and added to a report. Access to data for reporting purposes is restricted according to the role granted to the user (see above Section C.4). Below shows a list of the ad hoc reports created and stored in BDMIS.



Showing 20 at a time: Items 1-20 of 301

Options	Class ▾	Label ▾	Description ▾	Modified On ▴	Last Run
	Applicant	[applicant] / 2009-11-10 09:47:00		Nov 10, 2009 9:50 am	Nov 10, 2009, 10:00 am
	Applicant	[applicant] / 2009-10-30 15:05:49		Oct 30, 2009 3:12 pm	Oct 30, 2009, 3:38 pm
		temp	test	Oct 23, 2009 1:40 pm	-
	Applicant	[applicant] / 2009-10-21 13:48:23		Oct 21, 2009 1:43 pm	Oct 21, 2009, 1:51 pm
	Applicant	11 2009 408 11/04/2009		Oct 19, 2009 2:48 pm	Nov 4, 2009, 6:25 pm
	Applicant	11 Avg Age FOIA Request 10/19/2009		Oct 19, 2009 2:48 pm	Oct 19, 2009, 2:55 pm
	Applicant	[applicant] / 2009-08-31 16:03:34		Oct 16, 2009 11:59 am	Oct 16, 2009, 12:07 pm
	Applicant	[applicant] / 2009-08-04 17:27:19		Oct 14, 2009 9:34 am	Oct 14, 2009, 9:41 am
	Applicant	[applicant] / 2009-10-07 12:03:03		Oct 07, 2009 11:57 am	Oct 7, 2009, 12:05 pm
	Applicant	[applicant] / 2009-10-07 11:49:14		Oct 07, 2009 11:43 am	Oct 7, 2009, 12:01 pm
	Applicant	CF Find an Assignment	Find A BOS Assignment/Assigner	Oct 06, 2009 5:56 pm	Oct 6, 2009, 6:08 pm
	Applicant	LA AR 7-14-09	LA Annual Reviews 9-30-09	Sep 30, 2009 12:59 pm	Sep 30, 2009, 1:06 pm
	Applicant	[applicant] / 2009-09-29 15:20:32		Sep 30, 2009 11:08 am	Sep 30, 2009, 1:40 pm
	Applicant	[applicant] / 2009-09-28 17:15:37		Sep 29, 2009 9:23 am	Sep 29, 2009, 1:01 pm

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.

Individuals may decline to provide information or withhold their consent for particular uses of the information, but both are conditions for initial acceptance and continuing eligibility in the SBA 8(a) Business Development Program. All information is provided on a voluntary basis by the applicants. The information is used solely for the evaluation of the applicant for certification and/or continuing eligibility in the 8(a) program, so no consent for any other use is solicited.

11) Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used as intended.

The first layer of system security is provided by GLS, which ensures userid and password protected access from the intranet and internet. The second layer of security is provided by the complex role structure, described in Section C.4 above. These procedures are documented in system documentation available on demand. In addition, all SBA employees and assigned contractor staff receive SBA-mandatory privacy training on the use and disclosure of personal data. They also receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on SBA security policies and procedures.

All government and contractor personnel are vetted and approved access to the data center where the system is housed, issued picture badges, and given specific access to areas necessary to perform their job function. A rules of behavior document provides an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of the rules of behavior prior to getting access to any IT system.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is operated in a single site.

2) What are the retention periods of data in this system?

Retention of the information provided is indefinite. Upon completion of the 9 year term for participation in the 8(a) Business Development Program, all data relating to the participant is archived in the system for an indefinite period until such time as they are deemed inactive, at which time they will be retired or destroyed in accordance with records schedules of the United States Small Business Administration and as approved by the National Archives and Records Administration.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The procedures for disposition of the data at the end of the retention period are outlined in Chapter 5 of SBA SOP 00 41 02, ‘Records Management Program’, at this link:

http://www.sba.gov/sops/0041/sop0041.pdf

The data will be kept for an indefinite period, until deemed inactive by the Office of Business Development.

4) Is the system using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

The process is not new to the SBA. Precursor systems collected the same data and stored it electronically.

5) How does the use of this technology affect public/employee privacy?

N\A.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Each application in the system is tracked via an 'Action History' audit log, that records all procedural actions that affect a particular firm's application. Each action is accompanied by a corresponding date and the userid of the user that took the action. For example, when an application for 8(a) certification is approved by the Associate Administrator for Business Development (AABD), the action 'Approved by AABD' and the name and/or userid of the person in that role who took the action is also shown. Example?

7) What kinds of information are collected as a function of the monitoring of individuals?

BDMIS records every action in the system, along with the userid of the 'actor' and the time and date of the action. Invalid log-in attempts are recorded and stored in the GLS security front-end, which is maintained by the SBA OISS. Authentication and identification upon log-in are also controlled and tracked via the GLS security front-end.

8) What controls will be used to prevent unauthorized monitoring?

Employees or contractors are assigned roles for accessing the system based on their function. Access to data is limited to a specific subset on a 'need to know' basis for each role (see above). In addition, SBA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained on information security when they join the organization and periodically thereafter. The Information Systems Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

9) Under which Privacy Act systems of records notice (SORN) does the system operate? Provide number and name.

The system is described as 'SBA 30' in the following SORN from the Federal Register, dated April 1, 2009:

http://www.sba.gov/idc/groups/public/documents/sba_program_office/foia_sys_of_rec.pdf

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

This document serves to update the Privacy Act system of records notice.

F. DATA ACCESS

a. **Who will have access to the data in the system?** (e.g., contractors, users, managers, system administrators, developers, tribes, other)

The following user types will have access to data in the system:

1. The public:
   a. Socially and economically disadvantaged individuals applying for 8(a) Program certification for the firms they own.
   b. Individuals who own firms already certified in the 8(a) Program.
2. SBA Staff:
   a. System Administrator / Project Manager who monitors use of the system, and manages the 'bug' fixing process with the developer. Also manages the implementation of any enhancements to the system. This individual also assigns roles in the system to users of all types. This individual also runs reports on demand for senior management of the SBA.
   b. Central Office Duty Station (CODS) staff:
      i. Business Opportunity Specialist (BOS): Reviews on-line applications submitted by public individuals for eligibility in the 8(a) Program. Makes recommendation to approve or decline application.
      ii. CODS Chief: Reviews analysis and approval by BOS, and makes recommendation to support or reject the BOS's decision.
   c. Headquarters:
      i. Assistant Administrator for Certification and Eligibility (AACE): Reviews decision by CODS Chief and makes recommendation to approve or reject it.
      ii. Associate Administrator for Business Development (AABD): Reviews decision by AACE and makes recommendation to approve or reject it.
      iii. Office of General Counsel (OGC); Reviews selected applications and decisions based on the needs of the agency.

iv. Office of Hearing and Appeals (OHA): Reviews selected applications and decisions based on the needs of the agency.

v. Terminations staff: Reviews files for firms subject to termination from the 8(a) Program.

vi. FOIA staff: Runs reports on firms in the program cleared for FOIA release.

d. District Office:

i. Business Development Specialist (BDS): Analyzes and reviews the on-line 8(a) Program Annual Review documentation submitted by firms already in the program and in the geographic area of jurisdiction of the District Office. Makes recommendation to retain, graduate, suspend or terminate the firm.

ii. Assistant District Director for 8(a) (ADD): Reviews the analysis and decision of the BDS, and makes recommendation to support or veto it.

iii. District Director (DD): Reviews the decision of the ADD and makes recommendation to support or veto it.

3. Contractors (all with active Security Clearances):

a. Developers: Fixes bugs identified by the System Administrator/Project Manager, also develops and implements any formal enhancements to the system.

b. Data Base Manager: Deals with database issues concerning the system.

c. Project Manager: Vendor counterpart to the SBA Project Manager with regard to implementation of any enhancements to the system.

b. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is determined by:

1. SBA staff:

a. Depends on the user(s) role(s) in the certification and annual review processes, as defined by the relevant SOP (http://collab.sba.gov/sites/GCBD/OBD/SOPs/ch10sopRevised_001.PDF). This document fully documents the roles and responsibilities of the SBA staff involved in these processes.

b. Other SBA staff, e.g., FOIA and Terminations, are assigned roles per instructions from Program Office management.

2. Public users:

a. Firms applying for 8(a) certification: Access is limited to firms that are duly registered in the Central Contractor Registry database. This database is restricted to firms that are qualified to do business with the Federal Government. BDMIS checks to ensure that the firm applying for 8(a) status is duly registered in CCR before according the user access to the system.

b. Firms already certified in the 8(a) Program returning for their Annual Review: Only firms already certified in the program AND duly registered in CCR are allowed access to BDMIS.

b.Will users have access to all data on the system or will the user's access be restricted? Explain.

Access is restricted by role.

1. The public
   a. Socially and economically disadvantaged individuals applying for 8(a) Program certification for the firms they own: Each such individual has access ONLY to the information he/she enters in the system. He/she also has access ONLY to the password he/she has chosen to access this data.
   b. Individuals who own firms already certified in the 8(a) Program. Each such individual has access ONLY to the information he/she enters in the system. He/she also has access ONLY to the password he/she has chosen to access this data..
2. SBA Staff
   a. System Administrator / Project Manager who monitors use of the system, and manages the 'bug' fixing process with the developer. He/she also manages the implementation of any enhancements to the system. This individual also assigns roles in the system to users of all types. This individual also runs reports on demand for senior management of the SBA. This individual has access to ALL data in the system, EXCEPT the passwords used by any other user of the system. As a result, the Systems Administrator cannot log in as a different user, and 'mimic' activity by that user.
   b. Central Office Duty Station (CODS) staff:

      i. Business Opportunity Specialist (BOS): Reviews on-line applications submitted by public individuals for eligibility in the 8(a) Program. Makes recommendation to approve or decline application. This individual has access only to data for firms in the specific office code of the CODS. For example, all applications going to the San Francisco CODS are assigned automatically to office code 0912. The CODS staff in San Francisco can only see data for the firms assigned to that office code. By the same token, the firms going to the Philadelphia CODS are automatically assigned to office code 0303. CODS staff in Philadelphia can see data ONLY for firms assigned to that office code.

      ii. CODS Chief: Reviews analysis and approval by BOS, and makes recommendation to support or reject the BOS's decision. Data access is restricted same as for BOS above.
   c. Headquarters:

        i. Assistant Administrator for Certification and Eligibility (AACE): Reviews decision by CODS Chief and makes recommendation to approve or reject it. Can see data for all firms
        ii. Associate Administrator for Business Development (AABD): Reviews decision by AACE and makes recommendation to approve or reject it. Can see data for all firms
        iii. Office of General Counsel (OGC); Reviews selected applications and decisions based on the needs of the agency. Can only see data for firms referred to it by another HQ SBA staff role in BDMIS.
        iv. Office of Hearing and Appeals (OHA): Reviews selected applications and decisions based on the needs of the agency. Can only see data for firms referred to it by another HQ SBA staff role in BDMIS
        v. Terminations staff: Reviews files for firms subject to termination from the 8(a) Program. Can only see data for firms in the process of being terminated.
        vi. FOIA staff: Runs reports on firms in the program cleared for FOIA release. Can see data on an as needed basis for a give FOIA request.
    d. District Office:
        i. Business Development Specialist (BDS): Analyzes and reviews the on-line 8(a) Program Annual Review documentation submitted by firms already in the program and in the geographic area of jurisdiction of the District Office. Makes recommendation to retain, graduate, suspend or terminate the firm. Can only see data for firms serviced by his/her specific District Office (ie, office code).
        ii. Assistant District Director for 8(a) (ADD): Reviews the analysis and decision of the BDS, and makes recommendation to support or veto it. Can only see data for firms serviced by his/her specific District Office (ie, office code).
        iii. District Director (DD): Reviews the decision of the ADD and makes recommendation to support or veto it. Can only see data for firms serviced by his/her specific District Office (ie, office code).

3. Contractors (all with active Security Clearances):
    a. Developers: Fixes bugs identified by the System Administrator/Project Manager, also develops and implements any formal enhancements to the system. Can see data for all firms and users (but no individual user passwords).
    b. Data Base Manager: Deals with database issues concerning the system. Can see data for all firms and users (but no individual user passwords).
    c. Project Manager: Vendor counterpart to the SBA Project Manager with regard to implementation of any enhancements to the system. Can see data for all firms and users (but no individual user passwords).

c. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

All SBA employees are required to obtain a Public Trust Security Clearance (see OPM Form 85P for details), which includes an exhaustive background check conducted by specialized professionals. Direct access to the system is limited by User ID's and password controls managed via the SBA's General Login System. Access via GLS is provided by the SBA Office of IT security upon receipt of a written request by the user and duly approved by an authorized SBA manager. Further access to data, once the user is admitted to the system, is regulated via access roles and profiles associated with each User ID.

Each user is required to have a role in the certification and/or annual review workflow (Roles are defined below in Section 8.1 below), as well as an individual system profile. Access to data, screens, functions, and reports is a function of the user's role in the workflow and his/her individual profile. In addition, with the exception of executive level roles (such as System Administrator, Associate Administrator for Business Development, and Assistant Administrator for Certification), access to information for a given role is limited to a specific Office Code.

All users of the system are also required to take Computer Security Awareness training on an annual basis.

d. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, contractors are involved in the design, development, and maintenance of the system. These include three employees of the Symplicity Corporation: Robert Cissell (Developer), Alok Dhir (Database Manager) and Ariel Friedler (Project Manager). They were required to pass a rigorous background check and Security Clearance before gaining access to third party personal data (relevant contract clause is included below):

<u>SECURITY REGULATIONS</u>

Agency security regulations as well as the Federal Privacy Act of 1974 govern data contained within all SBA computer systems. Contractor personnel assigned to this project will be held accountable for adherence to these regulations.

The work to be performed is unclassified, but may involve data which is restricted under the Privacy and Freedom of Information Acts. However, as a condition for access to government-owned systems and data, contractor personnel must pass background investigations in accordance with OMB Circular A-130, which requires screening of all individuals involved with sensitive applications or data in Federal automated information systems. All SBA automated systems and data are considered sensitive.

The SBA or its designated representative will perform background investigations. Contractor personnel, depending upon the labor category, will be subjected to one of the following background investigations:

National Agency Check and Inquiries (NACI) which consists of:

- Searches of the OPM Security/Suitability Investigations Index (SII)
- Searches of the Defense Clearance and Investigations Index
- Searches of the FBI Identification Division, fingerprint charts and FBI records Management Division files and
- Written inquiries and record searches covering specific areas of a subject's background during the past 5 years.

Minimum Background Investigation (MBI) which consists of:

- National Agency Check and Inquiries (above)
- Personal Subject Interview and
- Credit search

e. Do other systems share data or have access to the data in the system? If yes, explain.

A nightly FTP feed of data is transmitted from BDMIS to the E8a System at the SBA. The data feeds certain fields in the latter system, which serves as a repository of data about firms in the Annual Review Process. The mapping of fields between the two systems is shown in requirements and control documents that are available on request.

f. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The System Owner has this responsibility.

g. Will other agencies share data or have access to the data in this system via transferred or transmitted (Federal, State, and Local, Other (e.g., Tribal)?

The 4506T form is filled out by the applicant and sent to the IRS for processing. This form is a 'Request for Transcript of Tax Return', and includes the following information about the applicant: name, spouse's name, both social security numbers, current address, name, address and telephone number of third party recipient of tax return (e.g., SBA).

h. How will the shared data be used by the other agency?

The data in the form is used by the IRS to provide a transcript of the applicant's Federal tax return to the 8(a) certifying unit of the SBA (CODS).

i. What procedures are in place for assuring proper use of the shared data?

The electronic 4506T form and the data it contains is maintained in BDMIS for an indefinite period of time, and is secured by the processes and procedures for data security outlined in this document and the current approved System Security Plan for BDMIS, on file with OCIO.

Paper copies of the 4506T for the firms in the 8a Program are maintained in secured and locked premises at the various SBA District Offices across the United States.

The IRS maintains among the highest standards of information privacy and security in the US Government, given the sensitivity of the data it collects.

j. Privacy Impact Analysis: Discuss what privacy risks were identified and how they were mitigated for information shared internal and external.

No privacy risks were identified, as the IRS is deemed to have one of the best protected data privacy and security environments in the US Government.

Privacy Impact Assessment PIA Approval Page

The Following Officials Have Approved this Document:

1) System Owner

_____________ (Signature) 5/18/10 (Date)

Name: CALVIN JENKINS

Title: Deputy, GCBD

2) Project Manager

_____________ (Signature) 05/18/2010 (Date)

Name: LAWRENCE A. GOTTLIEB

Title: Project Manager, BDMIS

3) IT Security Manager

_____________ (Signature) 5/20/10 (Date)

Name: Troy Thompson

Title: CISO (A)

4) Acting Chief Privacy Officer

_____________ (Signature) 6-16-10 (Date)

Name:

Title: